Statement of Frontier Communications Corporation
Regarding Proposed H.B. 6317
AN ACT ESTABLISHING PUBLIC-PRIVATE PARTNERSHIPS TO PROVIDE INTERNET SECURITY TRAINING AND EXERCISES
Before the Committee on Public Safety and Security Committee
February 17, 2015

Proposal:

Proposed House Bill 6317 was introduced to "account for the rising threats and attacks to computers, networks, data and programs and reduce the vulnerability of the infrastructure of this state to such attacks."

Comments:

Frontier Communications Corporation ("Frontier") appreciates the opportunity to provide comment on the proposed bill.

Cybersecurity is a critical part of our business: We view cybersecurity as central to our mission of protecting corporate and individual information and systems. We are continuously evolving our cybersecurity capabilities, embracing innovative new technologies and offering new services throughout our networks.

Frontier has been working on cybersecurity concerns as a regular practice for the past 30 years when local and remote access controls and methodologies were established for new digital switching equipment. Since that time, Frontier's cybersecurity practices have evolved and grown on a regular basis as updated or new equipment is added to the network, as new services are offered, and when new security issues arise.

The industry's current cybersecurity efforts go beyond our internal practices to include public-private partnerships with a focus on national security and emergency preparedness for the communications industry. Frontier is particularly attuned to this, as Frontier's CEO Maggie Wilderotter was – until recently – the Chair of the President's National Security Telecommunications Advisory Committee (NSTAC), which has the mission of providing industry advice to the U.S. Government on critical infrastructure issues. In addition to NSTAC, there are number of multidisciplinary and ongoing efforts at the federal level to address cybersecurity, in which Frontier participates.

For instance, industry is participating in the National Institute of Standards and Technology (NIST) effort, which brought together, through a year-long collaborative effort, hundreds of public and private sector experts. The mission of these experts was to develop, in partnership, a voluntary cybersecurity framework—based on existing standards, guidelines, and practices—that could be used by organizations to enhance their risk management capabilities.

Since the release of the NIST Cybersecurity Framework in 2014, over 100 professionals are engaged in a major effort through the Communications Security, Reliability and Interoperability

Council (CSRIC) to adapt the NIST Cybersecurity Framework to five segments within the broad Communications Sector. Representatives from the broadcast, cable, satellite, wireless and wireline segments are included in this effort and there is active participation by state commissioners (Commissioners Tipton from Iowa and Witmer from Pennsylvania, and the NARUC general counsel Brad Ramsay). The goal is to build upon the risk management approach reflected in the NIST Framework and tailor it to the five segment operating environments. The final work product is due in March 2015 and it is expected to have a significant impact on the evolution of the framework effort.

Frontier supports the NIST Cybersecurity Framework approach to cybersecurity for numerous reasons including that:

- It allows entities to select controls from all major frameworks as well as custom control sets that are specific to the entity. This flexibility allows companies to employ controls developed for any framework and apply them where necessary as well as exclude controls where they are not needed;
- It provides a basis for a common measurement of diverse programs;
- It provides State and Federal Regulatory agencies a single Framework in which to measure and assess all entities;
- It consolidates compliance reporting to a single, flexible framework but still allows oversight;
- It is the result of broad collaboration and support between private industries, public industries, and business sectors;
- It creates an "open" process that allows for inclusion of ideas and framework changes, as opposed to third-party/proprietary frameworks, which are often created in a black box;
- It gives entities the flexibility to develop a single security controls framework; and
- It allows entities to apply security controls based on business risk and maturity as opposed to frameworks that require that all security controls should be applied at the most mature state

Because of this comprehensive approach NIST has undertaken, under the direction of the high level of expert professionals engaged in this effort to adapt the NIST Framework for the entire communications sector, we believe this is the most rational and Industry consistent approach to addressing and formulating our Cybersecurity policies and strategies.

Frontier recognizes that states have an interest in cybersecurity and need to engage on this topic and understand the cybersecurity posture of organizations that operate within their borders. Today, there are various state and regional initiatives through state CIOs, state homeland security offices, state governors, and other evolving state fora. In fact, the states participated in the development of the NIST Cybersecurity Framework process. In addition, states participate in critical efforts at the federal level to facilitate greater state awareness and engagement. States are involved in other regional initiatives including law enforcement and intelligence through the regional fusion centers. For example, the states participate in the DHS Critical Infrastructure and

Partnership Advisory Council (CIPAC) through the State, Local, Tribal and Territorial Coordinating Council (SLTTCC).

Conclusion:

As a national company that operates in 28 states, Frontier is concerned about a business landscape that includes multiple differing and potentially conflicting cybersecurity standards, compliance activities and oversight mechanisms. For this reason, rather than develop another process or effort focused at the state level, Frontier encourages the Committee to explore ways to more fully engage in the federal efforts, which are more mature and include and address state interests.